

AN ERROR ESTIMATE FOR COUNTING S_3 -SEXTIC NUMBER FIELDS

TAKASHI TANIGUCHI AND FRANK THORNE

ABSTRACT. In this note, we prove a power-saving remainder term for the function counting S_3 -sextic number fields. We also give a prediction on the second main term.

We also present numerical data on counting functions for S_3 -sextic number fields. Our data indicates that our prediction is likely to be correct, and it also suggests the existence of additional lower order terms which we have not yet been able to explain.

1. STATEMENT

We call a sextic number field \tilde{K} S_3 -sextic if \tilde{K} is Galois over \mathbb{Q} with $\text{Gal}(\tilde{K}/\mathbb{Q})$ isomorphic to the symmetric group S_3 . Let $N_6^\pm(X; S_3)$ be the number of S_3 -sextic fields \tilde{K} with $0 < \pm \text{Disc}(\tilde{K}) < X$. The primary term of $N_6^\pm(X; S_3)$ was obtained in independent works of Belabas-Fouvry [2] and Bhargava-Wood [3], and in this article we prove the following power-saving remainder term.

Theorem 1.1. *We have*

$$(1.1) \quad N_6^\pm(X; S_3) = \frac{C^\pm}{12} \prod_p c_p \cdot X^{1/3} + O(X^{1/3-5/447+\epsilon}),$$

where $C^+ = 1, C^- = 3$, the product is over all primes, and

$$c_p = \begin{cases} (1 - p^{-1})(1 + p^{-1} + p^{-4/3}) & p \neq 3, \\ (1 - \frac{1}{3})(\frac{4}{3} + \frac{1}{3^{5/3}} + \frac{2}{3^{7/3}}) & p = 3. \end{cases}$$

Moreover, under a natural but rather strong *assumption* of uniformity estimates for certain counting functions of cubic fields, we obtain

$$(1.2) \quad N_6^\pm(X; S_3) = \frac{C^\pm}{12} \prod_p c_p \cdot X^{1/3} + \frac{4K^\pm \zeta(1/3)}{5\Gamma(2/3)^3} \prod_p k_p \cdot X^{5/18} + o(X^{5/18}),$$

where $K^+ = 1, K^- = \sqrt{3}$ and

$$k_p = \begin{cases} 1 + \frac{1}{p^{13/9}(1+p^{-1})} \left(1 - \frac{1}{p^{2/9}} - \frac{1}{p^{5/9}} - \frac{1}{p^{2/3}}\right) & p \neq 3, \\ \frac{1}{4} \left(\frac{11}{3} - \frac{1}{3^{2/3}} + \frac{1}{3^{8/9}} + \frac{2}{3^{13/9}} - \frac{1}{3^{14/9}} - \frac{2}{3^{19/9}}\right) & p = 3. \end{cases}$$

As in [3], we relate counting S_3 -sextic fields to counting non-cyclic cubic fields with certain local completions. These cubic fields may then be counted using our previous work [11]. We may obtain a power saving error term simply by quoting our previous results, but we improve on this by applying the methods used in the proofs in [11]. This amounts to computing the Fourier transform of a function related to these local completions, and this computation was essentially carried out in [10].

We also computed $N_6^\pm(X; S_3)$ numerically for X up to $5 \cdot 10^{18}$, and we present our computations at the end of the paper. Interestingly, our computations suggest that (1.2) is likely to be correct, but with additional lower order terms which we were not able to explain.

2. PROOF

For a non-cyclic cubic field K , let \tilde{K} denote its Galois closure. Then the map $K \mapsto \tilde{K}$ gives a canonical bijection between the set of isomorphism classes of non-cyclic cubic fields and the set of isomorphism classes of S_3 -sextic fields. Let us compare $\text{Disc}(K)$ and $\text{Disc}(\tilde{K})$. They have the same sign, and if we write

$$\text{Disc}(K) = \pm \prod p^{e_p(K)}, \quad \text{Disc}(\tilde{K}) = \pm \prod p^{e_p(\tilde{K})},$$

we have the following.

- Lemma 2.1.** (1) *If K is not totally ramified at p , then $e_p(\tilde{K}) = 3e_p(K)$.*
 (2) *If K is totally ramified at p and $p \neq 3$, then $e_p(\tilde{K}) = 2e_p(K) = 4$.*
 (3) *If K is totally ramified at $p = 3$, then $e_p(\tilde{K}) = 7, 8$ or 11 according as $e_p(K) = 3, 4$ or 5 .*

Proof. Equivalent statements appear in [2] and [3], and we give a proof for the convenience of the reader. Let $F = \mathbb{Q}(\sqrt{\text{Disc}(K)})$ be the quadratic resolvent field of K (equivalently, the unique quadratic subfield of \tilde{K}). We have the classical formula (see, e.g. Theorem 2.5.1 and Lemma 10.1.27 of [4])

$$(2.1) \quad \text{Disc}(\tilde{K}) = \text{Disc}(K)^2 \text{Disc}(F).$$

Therefore, for $p > 2$, $e_p(\tilde{K})$ is equal to $2e_p(K) + a$, where $a = 0$ or 1 depending on whether $e_p(K)$ is even or odd.

For $p = 2$, observe that 2 can ramify in F only if it ramifies in K . If $(2) = \mathfrak{p}_1^2 \mathfrak{p}_2$ in K , then in \tilde{K} , (2) must split into three ideals with ramification index 2 . Therefore 2 must ramify in F with $e_2(F) = e_2(K)$ so that $e_2(\tilde{K}) = 3e_2(K)$. If $(2) = \mathfrak{p}^3$ in K , then 2 is tamely ramified in K , and therefore \tilde{K} , so that (2) splits into two ideals of ramification index 3 in \tilde{K} . This implies that (2) is unramified in F , so that $e_2(\tilde{K}) = 2e_2(K)$. □

In particular, $e_p(K)$ determines $e_p(\tilde{K})$ uniquely except for the case $p = 2$ and $e_2(K) = 2$, while in this case $e_2(\tilde{K})$ is either 6 or 4 according as K is partially or totally ramified at 2 .

Let us briefly explain our approach. If we ignore the ramification over the prime 3 , then Lemma 2.1 implies

$$(2.2) \quad \text{Disc}(\tilde{K}) =^* r^{-2} \text{Disc}(K)^3,$$

where r is the product of all primes where K is totally ramified.¹ So if we denote by $N_3^\pm(X; r)$ the number of non-cyclic cubic fields K such that r is the product of all primes where K is totally ramified and that $0 < \pm \text{Disc}(K) < X$, then

$$(2.3) \quad N_6^\pm(X; S_3) =^* \sum_r N_3^\pm(r^{2/3} X^{1/3}; r).$$

Here the sum is over all square-free integers r . However, (2.3) may not be true because of the ramification at 3 , so we specify the completion A of K at 3 and count for each A .

Let A denote an étale cubic algebra over \mathbb{Q}_3 (i.e., a direct product of field extensions of \mathbb{Q}_3 whose degrees add to 3) and r a square-free integer coprime to 3 . Let $\mathcal{K}_3(A, r)$ be the set of non-cyclic cubic fields K satisfying (i) $K \otimes_{\mathbb{Q}} \mathbb{Q}_3 \cong A$, (ii) K is totally ramified at all prime divisors of r , and (iii) except for at 3 and prime divisors of r , K is not totally ramified. Let \tilde{A} be the sextic algebra over \mathbb{Q}_3 isomorphic to $\tilde{K} \otimes_{\mathbb{Q}} \mathbb{Q}_3$ for $K \in \mathcal{K}_3(A, r)$, which does not depend on K . Let $\text{Disc}_3(A)$ and $\text{Disc}_3(\tilde{A})$ be the 3 -parts of their discriminants; e.g., write $\text{Disc}(A) = u \text{Disc}_3(A)$, where u is a 3 -adic unit², and

¹We have starred equalities which are not actually true.

²Observe that $\text{Disc}(A)$ and u are only defined up to squares of 3 -adic units, but $\text{Disc}_3(A)$ is well defined.

similarly for $\text{Disc}(\tilde{A})$. Then for $K \in \mathcal{K}_3(A, r)$, instead of (2.2) we have

$$(2.4) \quad \text{Disc}(\tilde{K}) = r^{-2} \frac{\text{Disc}_3(\tilde{A})}{\text{Disc}_3(A)^3} \text{Disc}(K)^3.$$

It will be convenient to put $m_A := \text{Disc}_3(A)^3 / \text{Disc}_3(\tilde{A})$. Let $N_3^\pm(X; A, r)$ denote the number of $K \in \mathcal{K}_3(A, r)$ with $0 < \pm \text{Disc}(K) < X$. We will use a formula of the form

$$(2.5) \quad \begin{aligned} N_3^\pm(X; A, r) &= \eta_3(A) \eta(r) \prod_p (1 - p^{-2}) \frac{C^\pm}{12} X \\ &+ \theta_3(A) \theta(r) \prod_p \left(1 - \frac{p^{1/3} + 1}{p(p+1)} \right) \frac{4K^\pm \zeta(1/3)}{5\Gamma(2/3)^3} X^{5/6} + O(r^\alpha X^\beta). \end{aligned}$$

Here $\eta_3(A)$ and $\theta_3(A)$ are “local densities” of A computed in [11], η and θ are multiplicative functions satisfying

$$\eta(p) = \frac{1}{p^2(1+p^{-1})}, \quad \theta(p) = \frac{1}{p^2(1+p^{-2/3}+p^{-1}+p^{-4/3})}$$

for any prime p , and α, β are certain real constants. By Theorem 1.2 in [11], (2.5) is true with $\alpha = 40/23, \beta = 18/23 + \epsilon$ and this suffices to obtain (1.1) with a larger error term of $O(X^{1/3-5/744+\epsilon})$. In this paper, we improve the estimate as follows.

Theorem 2.2. *The formula (2.5) is true for $\alpha = 7/23 + \epsilon, \beta = 18/23 + \epsilon$.*

We postpone its proof to the next section, and continue the proof of (1.1) and (1.2). Let $N_6^\pm(X; A)$ be the number of S_3 -sextic fields \tilde{K} such that $K \otimes_{\mathbb{Q}} \mathbb{Q}_3 \cong A$. Then by (2.4),

$$(2.6) \quad N_6^\pm(X; A) = \sum_{3 \nmid r} N_3^\pm(r^{2/3} m_A^{1/3} X^{1/3}; A, r)$$

where the sum is over all square-free integers coprime to 3. Therefore, our results follow from (2.6), (2.5), and a computation, the details of which follow.

We choose Q and split this sum into $r < Q$ and $r \geq Q$. By [11, Lemma 3.4] we have the estimate $N_3^\pm(X; A, r) = O(r^{-2+\epsilon} X)$. Hence the latter sum is bounded by $O(Q^{-1/3+\epsilon} X^{1/3})$. On the other hand it is easy to see that

$$\begin{aligned} \sum_{3 \nmid r, r < Q} \eta(r) r^{2/3} &= \prod_{p \neq 3} (1 + \eta(p) p^{2/3}) + O(Q^{-1/3+\epsilon}), \\ \sum_{3 \nmid r, r < Q} \theta(r) r^{5/9} &= \prod_{p \neq 3} (1 + \theta(p) p^{5/9}) + O(Q^{-4/9+\epsilon}). \end{aligned}$$

We define

$$c_p := (1 + \eta(p) p^{2/3})(1 - p^{-2}), \quad k_p := (1 + \theta(p) p^{5/9}) \left(1 - \frac{p^{1/3} + 1}{p(p+1)} \right) \quad (p \neq 3),$$

which coincide with the constants given in Section 1. We also put

$$\eta'_3(A) := (1 - 3^{-2}) \eta_3(A) m_A^{1/3}, \quad \theta'_3(A) := \left(1 - \frac{3^{1/3} + 1}{3(3+1)} \right) \theta_3(A) m_A^{5/18}.$$

Then by (2.6) and (2.5), we have

$$(2.7) \quad \begin{aligned} N_6^\pm(X; A) &= \eta'_3(A) \prod_{p \neq 3} c_p \cdot \frac{C^\pm}{12} X^{1/3} + \theta'_3(A) \prod_{p \neq 3} k_p \cdot \frac{4K^\pm \zeta(1/3)}{5\Gamma(2/3)^3} X^{5/18} \\ &+ O(X^{\beta/3} \sum_{r < Q} r^{\alpha+2\beta/3}) + O(Q^{-1/3+\epsilon} X^{1/3}). \end{aligned}$$

The first O -term is $O(Q^{\alpha+2\beta/3+1}X^{\beta/3})$, and we choose $Q = X^{\frac{1-\beta}{3\alpha+2\beta+4}}$ to obtain an error of $O(X^{\frac{1}{3}(1-\frac{1-\beta}{3\alpha+2\beta+4})+\epsilon})$ in (2.7). With our constants $\alpha = 7/23 + \epsilon$ and $\beta = 18/23 + \epsilon$, this is $O(X^{\frac{1}{3}(1-\frac{5}{149})+\epsilon})$. If (2.5) is true for e.g., $\alpha = -1, \beta = 1/2$, this is $O(X^{1/4+\epsilon})$ and we would obtain the second main term. Such an estimate might be true, but it seems difficult to prove.

Recall that

$$N_6^\pm(X; S_3) = \sum_A N_6^\pm(X; A)$$

where A in the right hand side runs through all the étale cubic algebras over \mathbb{Q}_3 . (There are finitely many, as there are finitely many field extensions of \mathbb{Q}_3 of degree ≤ 3 .) Hence the contribution to the main term of $N_6^\pm(X; S_3)$ from the prime 3 is given by

$$c_3 := \sum_A \eta'_3(A) = (1 - 3^{-2}) \sum_A \eta_3(A) m_A^{1/3}.$$

The local density $\eta_3(A)$ is given in the tables in Section 6.2 of [11]. Also, m_A is equal to 1, 9, or 81 depending on whether the 3-adic valuation of $\text{Disc}(A)$ is less than 3, equal to 3, or greater than 3. We therefore compute that

$$(2.8) \quad c_3 = (1 - 3^{-2}) \cdot \frac{1 + \frac{1}{3} + \frac{2}{27} \cdot 3^{2/3} + \frac{1}{27} \cdot 3^{4/3}}{1 + \frac{1}{3}},$$

which is equal to the quantity given in Section 1. Similarly, the contribution to the secondary term is given by

$$(2.9) \quad \sum_A \theta'_3(A) = \left(1 - \frac{3^{1/3} + 1}{3(3+1)}\right) \sum_A \theta_3(A) m_A^{5/18},$$

and a similar calculation yields the value of k_3 given in Section 1.

3. PROOF OF THEOREM 2.2

In this section, we prove Theorem 2.2 by following the arguments of [10] and [11].

A brief sketch of our proof is as follows. In [11], we counted cubic fields in terms of contour integrals of certain zeta functions introduced by Shintani [9], associated to the space of *binary cubic forms*. Our method is naturally compatible with “local specifications” such as those appearing in (2.5), and the error terms of (2.5) depend on the “shape” of these local specifications. More precisely, they depend on the Fourier transforms of certain indicator functions associated to these local specifications. We establish fairly sharp bounds for these Fourier transforms on average, which lead to reasonably good bounds on the error terms in (2.5) (in α -aspect) and therefore in Theorem 1.1.

We follow the notations of [10] and [11], but recall the most basic ones. Let

$$(3.1) \quad V(\mathbb{Z}) := \{x = (x_1, x_2, x_3, x_4) = x_1 u^3 + x_2 u^2 v + x_3 u v^2 + x_4 v^3 \mid x_1, \dots, x_4 \in \mathbb{Z}\}$$

be the set of integral binary cubic forms. As in [10], [11], we consider the usual twisted action on $\text{GL}_2(\mathbb{Z})$ on $V(\mathbb{Z})$. Then it is known that there is a discriminant preserving bijection between $\text{GL}_2(\mathbb{Z}) \backslash V(\mathbb{Z})$ and the set of isomorphism classes of cubic rings.³

To define the zeta functions we study, we introduce several functions on $V(\mathbb{Z})$. Let $p \neq 3$ be a prime. Let Φ_p (resp. Ψ_p) be the indicator function on $V(\mathbb{Z})$ which detects those cubic rings which are nonmaximal or maximal but totally ramified (resp. maximal and totally ramified) at p . These two functions factor through the reduction map $V(\mathbb{Z}) \rightarrow V(\mathbb{Z}/p^2\mathbb{Z})$ modulo p^2 , and we use the same notation Φ_p, Ψ_p to denote these functions on $V(\mathbb{Z}/p^2\mathbb{Z})$. We fix an étale cubic algebra A over \mathbb{Q}_3 throughout this section.⁴ Let Φ_A be the function on $V(\mathbb{Z})$ which detects the cubic rings R such that

³Recall that a cubic ring is a commutative ring which is free of rank 3 as a \mathbb{Z} -module.

⁴Since there are finitely many A , uniformity in our error terms with respect to A is automatic.

$R \otimes \mathbb{Z}_3 \cong \mathcal{O}_A$ where \mathcal{O}_A is the integral closure⁵ of \mathbb{Z}_3 in A . This Φ_A factors through $V(\mathbb{Z}) \rightarrow V(\mathbb{Z}/27\mathbb{Z})$. As above, we use the same Φ_A to denote the function on $V(\mathbb{Z}/27\mathbb{Z})$.

Let r and q be square free integers satisfying $(q, r) = (qr, 3) = 1$. We put $\Phi_q = \prod_{p|q} \Phi_p$ and $\Psi_r = \prod_{p|r} \Psi_p$. These are either functions on $V(\mathbb{Z})$, or functions respectively on $V(\mathbb{Z}/q^2\mathbb{Z})$ and $V(\mathbb{Z}/r^2\mathbb{Z})$. With this preparation, we define the zeta functions

$$(3.2) \quad \xi_{r,q}^{\pm}(s) := \sum_{x \in \text{GL}_2(\mathbb{Z}) \backslash V(\mathbb{Z})} \Phi_A(x) \Psi_r(x) \Phi_q(x) \frac{|\text{Stab}(x)|^{-1}}{|\text{Disc}(x)|^s},$$

where the sign \pm indicates that the sum is over orbits of either positive or negative discriminants. As in [11], Theorem 2.2 follows from uniform estimates for the zeta functions $\widehat{\xi}_{r,q}^{\pm}(s)$ which are dual to $\xi_{r,q}^{\pm}(s)$. We now introduce these dual zeta functions $\widehat{\xi}_{r,q}^{\pm}(s)$, which are associated with the dual representation (G, V^*) .

Let V^* denote the dual of V . Then, by definition, $V^*(\mathbb{Z})$ is canonically isomorphic to the dual lattice $\text{Hom}(V(\mathbb{Z}), \mathbb{Z})$. We denote the canonical pairing, on V and V^* , by $[x, y]$ for $x \in V, y \in V^*$. We may and do consider the action on V^* such that $[gx, gy] = (\det g)[x, y]$ for $x \in V, y \in V^*$ and $g \in \text{GL}_2$. Then there is an invariant polynomial P^* on V^* such that $P^*(gy) = (\det g)^2 P^*(y)$. For details, see Section 2 in [10].

The (finite) Fourier transform of Ψ_r , which is a function on $y \in V^*(\mathbb{Z}/r^2\mathbb{Z})$, is defined by

$$(3.3) \quad \widehat{\Psi}_r(y) := \frac{1}{r^8} \sum_{x \in V(\mathbb{Z}/r^2\mathbb{Z})} \Psi_r(x) \exp\left(2\pi\sqrt{-1} \cdot \frac{[x, y]}{r^2}\right), \quad y \in V^*(\mathbb{Z}/r^2\mathbb{Z}).$$

We define $\widehat{\Phi}_A$ and $\widehat{\Psi}_q$ similarly. Then the dual zeta function is defined by

$$(3.4) \quad \widehat{\xi}_{r,q}^{\pm}(s) := \sum_{y \in \text{GL}_2(\mathbb{Z}) \backslash V^*(\mathbb{Z})} \widehat{\Phi}_A(y) \widehat{\Psi}_r(y) \widehat{\Phi}_q(y) \frac{|\text{Stab}(y)|^{-1}}{|P^*(y)/3^{12}r^8q^8|^s}.$$

Because of the functional equation

$$(3.5) \quad \begin{pmatrix} \xi_{r,q}^+(1-s) \\ \xi_{r,q}^-(1-s) \end{pmatrix} = \frac{3^{6s-2}}{2\pi^{4s}} \Gamma(s)^2 \Gamma\left(s - \frac{1}{6}\right) \Gamma\left(s + \frac{1}{6}\right) \begin{pmatrix} \sin 2\pi s & \sin \pi s \\ 3 \sin \pi s & \sin 2\pi s \end{pmatrix} \begin{pmatrix} \widehat{\xi}_{r,q}^+(s) \\ \widehat{\xi}_{r,q}^-(s) \end{pmatrix},$$

the estimate of the O -term in (2.5) is reduced to the study of these dual zeta functions $\widehat{\xi}_{r,q}^{\pm}(s)$. In particular, we need an estimate of them uniformly with respect to r and q . We write

$$(3.6) \quad \widehat{\xi}_{r,q}^{\pm}(s) := \sum_{\mu_n} \frac{c_{r,q}^{\pm}(\mu_n)}{\mu_n^s}.$$

Hence the sum is over $\mu_n \in \frac{1}{3^{12}r^8q^8}\mathbb{Z}$. We fix a choice of sign and drop \pm from our notation. The following bound essentially follows from Theorem 4.1 in [11].

Proposition 3.1. *For any fixed $\epsilon > 0$, we have the bounds*

$$(3.7) \quad \sum_{\mu_n < X} |c_{r,q}(\mu_n)| \ll (rq)^{2+\epsilon} X,$$

$$(3.8) \quad \sum_{\mu_n < X} |c_{r,q}(\mu_n)| \ll (rq)^{1+\epsilon} X + (rq)^{-1+\epsilon},$$

uniformly for all r, q and X .

⁵If A is of the form $A = \prod A_i$ where A_i/\mathbb{Q}_3 are field extensions, then $\mathcal{O}_A = \prod \mathcal{O}_{A_i}$ where each \mathcal{O}_{A_i} is the integer ring of A_i .

Proof. In [10], we gave the explicit formulas of the Fourier transforms $(\Phi_p - \Psi_p)^\wedge = \widehat{\Phi_p} - \widehat{\Psi_p}$ and $\widehat{\Phi_p}$ in Theorems 6.3 and 6.4, respectively. Hence the explicit formula of $\widehat{\Psi_p}$ follows as well. We introduce a function Φ_p^* on $V^*(\mathbb{Z}/p^2\mathbb{Z})$ by

$$(3.9) \quad \Phi_p^*(b) = \begin{cases} p^{-5} & b \text{ is of type } (1_{\max}^3), \\ |\widehat{\Phi_p}(b)| & \text{otherwise.} \end{cases}$$

Then we have $|\widehat{\Phi_p}| \leq \Phi_p^*$ and $|\widehat{\Psi_p}| \leq (1 + p^{-2})\Phi_p^*$. Let $c = \prod_p(1 + p^{-2})$. Note the trivial bound $|\widehat{\Phi_A}| \leq 1$. Therefore $\widehat{\xi_{r,q}^\pm}(s)$ is bounded coefficientwise by

$$(3.10) \quad \sum_{y \in \mathrm{GL}_2(\mathbb{Z}) \setminus V^*(\mathbb{Z})} c \Phi_{rq}^*(y) \frac{|\mathrm{Stab}(y)|^{-1}}{|P^*(y)/3^{12}r^8q^8|^s}.$$

Here $\Phi_{rq}^* = \prod_{p|rq} \Phi_p^*$. If $\Phi_{rq}^*(y)$ in above were replaced with $|\widehat{\Phi_{rq}}(y)|$, then (3.10) is, in the notation of Section 4 in [11], given by

$$(3.11) \quad c \sum_{\mu_n} \frac{b_{rq}(\mu_n)}{(\mu_n/3^{12})^s}.$$

So the bounds of this proposition follow from Theorem 4.1 in [11]. Our actual (3.10) is slightly different from (3.11) because of (3.9), but we can nevertheless easily modify the proof of Theorem 4.1 in [11] for our case and obtain the same estimate. We omit the detail. \square

Similarly to Proposition 4.2 in [11], we have the following corollary.

Proposition 3.2. *Let $z \geq r^{-2}q^{-2}$. For a fixed $0 < \delta < 1$ (and $\epsilon > 0$), we have the bounds*

$$(3.12) \quad \sum_{\mu_n < z} |c_{r,q}(\mu_n)|/\mu_n^\delta \ll (rq)^{3\delta-1+\epsilon} + (rq)^{1+\epsilon}z^{1-\delta}.$$

We also have, for any fixed $\delta > 1$,

$$(3.13) \quad \sum_{\mu_n > z} |c_{r,q}(\mu_n)|/\mu_n^\delta \ll (rq)^{1+\epsilon}z^{1-\delta}.$$

We are ready to prove Theorem 2.2.

Proof of Theorem 2.2. From exactly the same argument as of Section 5.3 in [11], the difference of the counting functions and the corresponding two main terms in (2.5) are, for any parameter $Q \leq X$ and $y \geq X^{3/5}$, bounded by

$$(3.14) \quad \ll \sum_{q < Q} E_q(r, y, X) + y^{1+\epsilon} + X/Q^{1-\epsilon},$$

where

$$(3.15) \quad E_q(r, y, X) = X^{3/8} \sum_{\mu_n < z_q} \frac{|c_{r,q}(\mu_n)|}{\mu_n^{5/8}} + X^{3/8} \left(\frac{X^3}{y^4} \right)^{\rho/4} \sum_{\mu_n \geq z_q} \frac{|c_{r,q}(\mu_n)|}{\mu_n^{5/8+\rho/4}}.$$

Here $\rho \geq 3$ is a positive integer and z_q is another parameter which we can choose freely for each q . By Proposition 3.2, for $z_q \geq r^{-2}q^{-2}$,

$$(3.16) \quad E_q(r, y, X) \ll X^{3/8} r^{7/8+\epsilon} q^{7/8+\epsilon} + X^{3/8} r^{1+\epsilon} q^{1+\epsilon} z_q^{3/8} + X^{3/8} r^{1+\epsilon} q^{1+\epsilon} z_q^{3/8} \left(\frac{X^3}{y^4 z_q} \right)^{\rho/4}.$$

For q satisfying $X^3/y^4 \geq r^{-2}q^{-2}$, we choose $z_q = X^3/y^4$ and get the bound

$$(3.17) \quad E_q(r, y, X) \ll X^{3/8} r^{7/8+\epsilon} q^{7/8+\epsilon} + X^{3/2} r^{1+\epsilon} q^{1+\epsilon} y^{-3/2}.$$

If $X^3/y^4 \leq r^{-2}q^{-2}$, we choose $z_q = r^{-2}q^{-2}$. Then $\frac{X^3}{y^4 z_q} \leq 1$, and so the latter two terms in the right hand side of (3.16) are bounded by the first, so that (3.17) holds for such q as well. Hence (3.14) is

$$(3.18) \quad \ll X^{3/8} r^{7/8+\epsilon} Q^{15/8+\epsilon} + X^{3/2} r^{1+\epsilon} Q^{2+\epsilon} y^{-3/2} + y^{1+\epsilon} + X/Q^{1-\epsilon}.$$

Our theorem follows by choosing $y = X/Q$ and $Q = X^{5/23} r^{-7/23}$. \square

4. REMARKS

We give some remarks. First, we counted S_3 -sextic fields \tilde{K} with specifying the 3-adic completion A of K , and by the same method we may specify any finite number of local completions of K . In particular for a fixed prime $p \neq 3$, the ratio of the contributions of S_3 -sextic fields whose splitting type of p is (111111), (222), (33), $(1^2 1^2 1^2)$ and $(1^3 1^3)$ for the first and second main terms of (1.2) are respectively given by

$$\frac{1}{6} : \frac{1}{2} : \frac{1}{3} : \frac{1}{p} : \frac{1}{p^{4/3}} \quad \text{and} \quad \frac{1 + \frac{2}{p^{1/3}} + \frac{1}{p^{2/3}}}{6} : \frac{1 + \frac{1}{p^{2/3}}}{2} : \frac{1 - \frac{1}{p^{1/3}} + \frac{1}{p^{2/3}}}{3} : \frac{1 + \frac{1}{p^{1/3}}}{p} : \frac{1}{p^{13/9}}.$$

For $p = 3$ the last term should be replaced by $3^{-5/3} + 2 \cdot 3^{-7/3}$ and $3^{-17/9} + 2 \cdot 3^{-22/9}$ respectively. For the splitting types $(1^2 1^2 1^2)$ and $(1^3 1^3)$ there are often multiple possibilities for $K \otimes \mathbb{Q}_p$, depending on p , and the terms above can be further subdivided following the tables in Section 6.2 of [11]. Note that for any p the sum of the first three entries (corresponding to fields unramified at p) is 1 and $1 + p^{-2/3}$ respectively.

Second, by the same method, we can prove the analogue of power-saving remainder term (1.1) over an arbitrary base number field F . We use the generalization of (2.5) over F , whose proof will appear elsewhere. The exponent of X in the O -term depends (only) on the degree $[F : \mathbb{Q}]$.

5. NUMERICAL EXPERIMENTS

Finally, we compared our result (1.2) for $N_6^\pm(X; S_3)$ to numerical data.⁶ Our data weakly confirms (1.2), but it suggests the presence of one or more additional secondary terms, perhaps of order $X^{1/4}$. At present, we do not have a satisfactory explanation for these apparent additional terms, and we would be most interested to see one!

We tabulated a list of all S_3 -sextic fields \tilde{K} with $|\text{Disc}(\tilde{K})| < 5 \cdot 10^{18}$. We began by using Belabas's cubic program [1] to generate a list of all cubic fields K with $|\text{Disc}(K)| < (5/3)^{1/2} 10^9$, including generating polynomials. We have $\text{Disc}(\tilde{K}) = \text{Disc}(K)^2 |\text{Disc}(F)|$, where F is the quadratic resolvent of K , and as $|\text{Disc}(F)| \geq 3$ we were able to tabulate S_3 -fields with discriminant bounded by $5 \cdot 10^{18}$. (We also obtained many fields \tilde{K} with larger discriminant, which we discarded.)

We used Lemma 2.1 to compute $\text{Disc}(\tilde{K})$ in terms of $\text{Disc}(K)$. In particular, $\text{Disc}(\tilde{K})$ is determined by $\text{Disc}(K)$ apart from the power of 2, which depends on whether or not K is totally ramified at 2. For the power of 2, Belabas's program outputs a binary cubic form $f = au^3 + bu^2v + cuv^2 + dv^3$ which corresponds to the maximal order \mathcal{O}_K , and 2 is totally ramified in K if and only if f has a triple root (mod 2), i.e., if

$$(5.1) \quad (a, b, c, d) \pmod{2} \in \{(1, 1, 1, 1), (1, 0, 0, 0), (0, 0, 0, 1)\}.$$

We used this condition to check the ramification at 2 and therefore to compile our list of S_3 -sextic extensions.

Finally, we compared our data to the two main terms of (1.2). The tables below list $N_6^\pm(X; S_3)$ for a variety of values of X between 10^{12} and 10^{19} . The columns (1.2) give the values predicted by (1.2),

⁶Our computer programs, as well as more detailed data on counts of S_3 -sextic extensions, are available for download from the second author's website. We wrote a Java program to parse the output of Belabas's `cubic` program and count S_3 -sextic extensions, and a PARI/GP [8] program to compute (1.2). To reproduce our results, it is also necessary to download and run Belabas's software; the output of his program is extremely large and cannot reasonably be made available.

which are consistently too high. (The bare main terms of Theorem 1.1 are still higher.)

| X | $N_6^+(X; S_3)$ | (1.2) | (5.4) | Error | X | $N_6^-(X; S_3)$ | (1.2) | (5.4) | Error |
|-------------------|-----------------|--------|--------|-------|-------------------|-----------------|--------|--------|-------|
| $1 \cdot 10^{12}$ | 690 | 756 | 709 | .031 | $1 \cdot 10^{12}$ | 2809 | 2979 | 2828 | .079 |
| $1 \cdot 10^{13}$ | 1650 | 1762 | 1682 | .027 | $1 \cdot 10^{13}$ | 6315 | 6613 | 6362 | .073 |
| $5 \cdot 10^{13}$ | 2984 | 3154 | 3038 | .027 | $5 \cdot 10^{13}$ | 11116 | 11517 | 11159 | .063 |
| $1 \cdot 10^{14}$ | 3848 | 4045 | 3910 | .025 | $1 \cdot 10^{14}$ | 14121 | 14617 | 14199 | .064 |
| $2 \cdot 10^{14}$ | 4981 | 5182 | 5025 | .021 | $2 \cdot 10^{14}$ | 17888 | 18545 | 18057 | .070 |
| $5 \cdot 10^{14}$ | 6948 | 7181 | 6987 | .019 | $5 \cdot 10^{14}$ | 24584 | 25390 | 24791 | .067 |
| $1 \cdot 10^{15}$ | 8867 | 9181 | 8955 | .021 | $1 \cdot 10^{15}$ | 31276 | 32192 | 31492 | .062 |
| $2 \cdot 10^{15}$ | 11324 | 11729 | 11464 | .023 | $2 \cdot 10^{15}$ | 39589 | 40803 | 39985 | .068 |
| $5 \cdot 10^{15}$ | 15740 | 16197 | 15870 | .020 | $5 \cdot 10^{15}$ | 54260 | 55798 | 54792 | .067 |
| $1 \cdot 10^{16}$ | 20062 | 20658 | 20276 | .021 | $1 \cdot 10^{16}$ | 68972 | 70683 | 69507 | .061 |
| $2 \cdot 10^{16}$ | 25578 | 26333 | 25885 | .022 | $2 \cdot 10^{16}$ | 87462 | 89519 | 88143 | .061 |
| $5 \cdot 10^{16}$ | 35337 | 36260 | 35708 | .021 | $5 \cdot 10^{16}$ | 119761 | 122290 | 120598 | .058 |
| $1 \cdot 10^{17}$ | 45054 | 46159 | 45513 | .021 | $1 \cdot 10^{17}$ | 151877 | 154800 | 152820 | .055 |
| $2 \cdot 10^{17}$ | 57403 | 58730 | 57973 | .021 | $2 \cdot 10^{17}$ | 192486 | 195914 | 193597 | .054 |
| $5 \cdot 10^{17}$ | 78905 | 80690 | 79756 | .022 | $5 \cdot 10^{17}$ | 263268 | 267402 | 264549 | .050 |
| $1 \cdot 10^{18}$ | 100335 | 102555 | 101460 | .022 | $1 \cdot 10^{18}$ | 333398 | 338279 | 334938 | .049 |
| $2 \cdot 10^{18}$ | 127924 | 130291 | 129007 | .020 | $2 \cdot 10^{18}$ | 422044 | 427869 | 423956 | .048 |
| $3 \cdot 10^{18}$ | 147249 | 149846 | 148436 | .019 | $3 \cdot 10^{18}$ | 484667 | 490869 | 486576 | .046 |
| $4 \cdot 10^{18}$ | 162478 | 165462 | 163956 | .020 | $4 \cdot 10^{18}$ | 534257 | 541099 | 536515 | .047 |
| $5 \cdot 10^{18}$ | 175624 | 178679 | 177094 | .020 | $5 \cdot 10^{18}$ | 576204 | 583564 | 578740 | .047 |

As there is an apparent discrepancy between the data and (1.2), we tried an amended heuristic. If $|\text{Disc}(\tilde{K})| < X$, then K cannot be totally ramified at any prime $> X^{1/4}$. This suggests multiplying the main term by a factor

$$(5.2) \quad \prod_{p > X^{1/4}} \frac{1 + p^{-1}}{1 + p^{-1} + p^{-4/3}} \sim 1 - \sum_{p > X^{1/4}} p^{-4/3} \sim 1 - \int_{X^{1/4}}^{\infty} \frac{t^{-4/3}}{\log t} \sim 1 - \frac{12X^{-1/12}}{\log X}.$$

(The approximations above are rather simple, so we verified numerically (for $X = 10^{18}$) that improving any of them leads only to minor differences.) Similarly, for the secondary term we incorporate the correction term

$$(5.3) \quad \prod_{p > X^{1/4}} \frac{1 + p^{-2/3} + p^{-1} + p^{-4/3}}{1 + p^{-2/3} + p^{-1} + p^{-4/3} + p^{-13/9}} \sim 1 - \sum_{p > X^{1/4}} p^{-13/9} + O(p^{-19/9}) \sim 1 - 9 \frac{X^{-1/9}}{\log X}.$$

This suggests the asymptotic formula

$$(5.4) \quad N_6^{\pm}(X; S_3) \sim \frac{C^{\pm}}{12} \prod_p c_p \cdot X^{1/3} \left(1 - \int_{X^{1/4}}^{\infty} \frac{t^{-4/3}}{\log X} \right) + \frac{4K^{\pm}\zeta(1/3)}{5\Gamma(2/3)^3} \prod_p k_p \cdot X^{5/18} \left(1 - 9 \frac{X^{-1/9}}{\log X} \right)$$

With these corrections, we obtained the values listed under (5.4) in our tables. These values are more accurate, but still do not seem to closely match the data.

The final column labeled ‘Error’ gives the relative error estimate $\frac{(1.2) - N_6^{\pm}(X, S_3)}{X^{5/18}}$. This column suggests that the secondary term in (1.2) is likely to be relevant, but the evidence is not overwhelming. There is, of course, a qualitative difference between the two sets of data as well: the relative error is lower in the positive discriminant case, but seems to be decreasing very slowly (if at all).

We tried other variations of these heuristics as well. As described earlier, we experimented with improving the estimates in (5.2) and (5.3) (e.g. evaluating the integrals in (5.2) and (5.3) numerically instead of using the approximation $\log t \sim \log X$ and evaluating them). This made only a very minor difference, and it adjusted our counts upward rather than downward. Also, we observed that in fact no prime larger than $\frac{X}{\sqrt[4]{3}}$ can totally ramify (as an S_3 -sextic field has a nontrivial quadratic resolvent), and we tried an accordingly modified version of (5.2) and (5.3). These modified heuristics still produced data which were too high.

Arithmetic progressions. Our work in [11] found and explained interesting discrepancies in the distribution of cubic field discriminants in arithmetic progressions. For example, the following table lists the number of cubic fields K with $0 < \text{Disc}(K) < 2 \cdot 10^6$ and $\text{Disc}(K) \equiv a \pmod{m}$ for $m = 5$ and 7. The “predicted” row is the sum of the X and $X^{5/6}$ terms of the asymptotic formula proved in [11].

| Discriminant modulo 5 | | 0 | 1 | 2 | 3 | 4 |
|-----------------------|--|-------|-------|-------|-------|-------|
| Actual count | | 21277 | 22887 | 22751 | 22748 | 22781 |
| Predicted | | 21307 | 22757 | 22757 | 22757 | 22757 |

| Discriminant modulo 7 | | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|-----------------------|--|-------|-------|-------|-------|-------|-------|-------|
| Actual count | | 15330 | 17229 | 14327 | 15323 | 17027 | 18058 | 15150 |
| Predicted | | 15316 | 17209 | 14277 | 15316 | 17024 | 18063 | 15131 |

The results (mod 5) could have been predicted by Davenport and Heilbronn [7]. In contrast, the $X^{5/6}$ term of the asymptotic is different for every residue class $a \pmod{7}$. We proved this in [11]; these results are explained by the existence of nontrivial sextic characters (mod 7), a phenomenon that could have been predicted earlier by Datskovsky and Wright [6].

We briefly investigated analogous questions for S_3 -sextic field discriminants, and we quickly found interesting behavior which our methods could not explain.

For example, S_3 -sextic field discriminants seem to not be equidistributed modulo 5! We computed the following data for S_3 -sextic fields \tilde{K} of negative discriminant (where there are no cyclic cubic fields), unramified at 2 and 3 (to eliminate wild ramification), and with $0 < -\text{Disc}(\tilde{K}) < X$:

| X | 0 | 1 | 2 | 3 | 4 |
|---------------------|-------|-------|-------|-------|-------|
| 10^{12} | 204 | 168 | 145 | 170 | 152 |
| 10^{13} | 439 | 388 | 344 | 365 | 368 |
| 10^{14} | 1010 | 848 | 788 | 845 | 811 |
| 10^{15} | 2288 | 1853 | 1773 | 1885 | 1780 |
| 10^{16} | 5034 | 4075 | 4027 | 4091 | 3974 |
| 10^{17} | 11211 | 9075 | 8833 | 8967 | 8817 |
| 10^{18} | 24816 | 19902 | 19395 | 19872 | 19530 |
| $3 \cdot 10^{18}$ | 36151 | 28939 | 28462 | 29031 | 28476 |
| 10^{17} | 11767 | 9249 | 9249 | 9249 | 9249 |
| $(3 \cdot 10^{18})$ | 37405 | 29421 | 29421 | 29421 | 29421 |

The last two rows are predictions from (1.2), modified as described in Section 4 for the primes 2, 3, and 5. For $p = 5$ the 0 column is the contribution from fields ramified at 5; the remainder is divided into four equal parts, as predicted by our methods above and in [11].⁷

The surplus of discriminants divisible by 5 is predicted by Lemma 2.1: for any cubic field K totally ramified at 5, we know that $\text{Disc}(\tilde{K}) \leq \frac{1}{25}\text{Disc}(K)^3$, and so many such fields have small discriminant. However, we were surprised to observe a surplus of field discriminants $\equiv 1, 3 \pmod{5}$. Certainly this

⁷In particular, the secondary terms of counting functions for cubic field discriminants, twisted by nontrivial Dirichlet characters (mod 5), vanish; see Section 6.4 of [11].

is not predicted by any analysis involving the Shintani zeta function. We looked for other heuristic explanations, for example using the fact that

$$(5.5) \quad \text{Disc}(\tilde{K}) \equiv (p_1 p_2 \dots p_m)^{-1} \pmod{5},$$

where $p_1, p_2, \dots, p_m > 5$ are the primes ramified but not totally ramified in K , but we found nothing explaining the apparent biases $\pmod{5}$.

In conclusion, (1.2) and probably also its generalization to arithmetic progressions, appear to be correct – but our experiments have uncovered additional phenomena which call for explanation. Naturally we hope to see further work on this topic in the future!

REFERENCES

- [1] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237; accompanying software available at <http://www.math.u-bordeaux1.fr/~belabas/research/software/cubic-1.2.tgz>.
- [2] K. Belabas and E. Fouvry. Discriminants cubiques et progressions arithmétiques, *Int. J. of Number Theory*, 6:1491–1529, 2010.
- [3] M. Bhargava and M. Wood. The density of discriminants of S_3 -sextic number fields. *Proc. Amer. Math. Soc.*, 136:1581–1587, 2008.
- [4] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, New York, 1999.
- [5] H. Cohen, Diaz Y Diaz, and M. Olivier. Counting discriminants of number fields. *J. Th. Nombres Bordeaux.*, 18:573–593, 2006.
- [6] B. Datskovsky and D. Wright, *The adelic zeta function associated to the space of binary cubic forms. II. Local theory*, J. Reine Angew. Math. **367** (1986), 27–75.
- [7] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.
- [8] PARI/GP, version 2.5.1, Bordeaux, 2012, available from <http://pari.math.u-bordeaux.fr/>.
- [9] T. Shintani, *On Dirichlet series whose coefficients are class numbers of integral binary cubic forms*, J. Math. Soc. Japan **24** (1972), 132–188.
- [10] T. Taniguchi and F. Thorne. Orbital L functions for the space of binary cubic forms. preprint, 2011.
- [11] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. preprint 2011, arXiv:1102.2914.

DEPARTMENT OF MATHEMATICS, GRADUATE SCHOOL OF SCIENCE, KOBE UNIVERSITY, 1-1, ROKKODAI, NADA-KU, KOBE 657-8501, JAPAN

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, FINE HALL, WASHINGTON ROAD, PRINCETON, NJ 08540
E-mail address: tani@math.kobe-u.ac.jp

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTH CAROLINA, 1523 GREENE STREET, COLUMBIA, SC 29208
E-mail address: thorne@math.sc.edu